

<b>Notice of Allowability</b>	<b>Application No.</b>	<b>Applicant(s)</b>
	10/021,042	KAMINAGA ET AL
	Examiner Samson B. Lemma	Art Unit 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS. This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.  This communication is responsive to 08/02/2005.
2.  The allowed claim(s) is/are 5-15 and 21-28.
3.  The drawings filed on 19 December 2001 are accepted by the Examiner.
4.  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a)  All
  - b)  Some\*
  - c)  None
  1.  Certified copies of the priority documents have been received.
  2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3.  Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5.  A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6.  CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
  - (a)  including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
    - 1)  hereto or 2)  to Paper No./Mail Date \_\_\_\_\_.
  - (b)  including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7.  DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

#### Attachment(s)

- |  |  |
|--|--|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892)   | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)            |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                 | 6. <input type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date _____. |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),<br>Paper No./Mail Date _____. | 7. <input type="checkbox"/> Examiner's Amendment/Comment                               |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material           | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance   |
|  | 9. <input type="checkbox"/> Other _____.   |

## ***DETAILED ACTION***

1. **Claims 1-4 and 16-20** have been cancelled.
2. **Claim 5** has been amended.
3. **New claims 21-28** have been added.

### ***Allowable Subject Matter***

4. **Claims 5-15 and 21-28** are allowed.
5. The following is an examiner's statement of reasons for allowance:
6. With respect to **the independent claims 5, 21 and 25** the art on the record, namely **Ohki and/or Kaisha** discloses all the limitation of the recited cancelled claims 1-4 and 16-20. Furthermore **Ohki and/or Kaisha** disclose/s the method/apparatus/or a software product for countering unauthorized decryption comprises a step of scrambling at least one correlation between a data decryption processing in a hardware and at least one respective hardware operation phenomenon by randomly changing at least one arithmetic operation order in the data decryption processing.

However, the art on the record does not disclose or suggest the limitation of the respective independent claims 5, 21 and 25, that has a functional limitation showing the method of scrambling the correlation by an arithmetic operation implemented by an information processing apparatus with respect to claim 5 or the specific method of calculating a value of a function in an encryption/decryption process with respect to claims 21 and 25 comprising the specific steps that has been recited in the independent claims 5, 21 and 25.

None of the prior art of record taken singularly or in combination teaches or suggests the specific steps that has been used in the respective independent claims to scramble the correlation by an arithmetic operation method implemented by an information processing apparatus and a specific method that has been used for calculating a value of a function in an encryption/decryption process.

For the reasons provided above, the amended independent claims 5, and the newly added independent claims 21 and 25 are allowed.

7. The dependent claims, being further limiting to the independent claims, definite and enabled by the specification are also allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "Comments on Statement of Reasons for Allowance."

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on. The fax phone number for the organization where this application or proceeding is assigned is 571-272-3799.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.  
08/17/2005

*Gilbert Barron Jr.*  
GILBERTO BARRON JR.  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100